UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/258,302	02/26/1999	MASAYUKI INOUE	501.36884X00	3656

20457 7590 11/03/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER	
LASTRA, DANIEL	

ART UNIT	PAPER NUMBER
3622	

DATE MAILED: 11/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/258,302	Applicant(s) INOUE ET AL.	
	Examiner DANIEL LASTRA	Art Unit 3622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 21-44 have been examined. The Application 09/258,302 **(POINT MANAGEMENT SYSTEM)** has a filing date 2/26/1999 and foreign priority of 03/03/1998.

Response to Amendment

2. In response to Final Office Action dated 05/05/04, the Applicant filed an RCE. Applicant amended claims 21-28, 38, 39 and 42. No new claims were added.

Claim Objections

3. Claims 24 and 25 are objected to because of the following informalities: "areas area" should read "area". Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 21-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takaragi et al (U.S. 4,885,788) in view of Mori et al (U.S. 5,659,166).

As per claim 21, Takaragi et al teach:

A point management system comprising:

a point system management apparatus for registering information of a store which participates in a point system, and for providing the store with a register store number for identifying the store and a crypt key of the store for encrypting data, both of said register store number and said crypt key of the store being peculiar to the store (see column 2, lines 1-25; see column 3, lines 59-65). Takaragi does not expressly mention a register store number corresponding to a store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not allowed to make reference to the transactions of other stores. And lines 59-67 of column 3 and figure 6, item 117 teach that each transaction area has a different authentication code that is used by each store to access its specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of

ordinary skill in the art at the time the application was made, to know that each transaction area would have a unique authentication code that would function as the registered store number corresponding to a store. This feature, in combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from the other stores.

Takaragi teaches an IC card that has a memory having a plurality of storage areas, each of said point storage areas storing point data, which is assigned corresponding to a customer's use, and a point management application, having a crypt key corresponding to said crypt key of the store, for processing data, including point data encrypted by said crypt key of the store, using said crypt key of said point management application, and for managing access to a point storage area corresponding to the store based on a register store number corresponding to the store and a reading and writing apparatus which reads and writes said IC card by using said register store number and said crypt key of the store *wherein each point storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key* (see column 2, lines 1-17; column 3, lines 59-65, column 8, lines 25-31). Takaragi does not teach the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically judged, and the predetermined number of points is converted into a number, which is

then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Takaragi IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 22, Takaragi et al teach:

An IC card comprising:

a memory having a plurality of point storage areas, each of said point storage areas storing point data which is assigned corresponding to a customer's use by a store which is assigned a register store number for identifying the store and a crypt key, of the store for encrypting data, both of said register store number and said crypt key of the store being peculiar to said store *wherein each point storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key* (see column 2, lines 1-25; see column 3, lines 59-65). Takaragi does not expressly mention a register store number corresponding to a store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not allowed to make reference to the transactions of other stores. And

lines 59-67 of column 3 and figure 6, item 117 teach that each transaction area has a different authentication code that is used by each store to access their specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that each transaction area has a unique authentication code that would function as the register store number corresponding to a store. This feature, in combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from the other stores.

Takaragi teaches a management application, having a crypt key corresponding to said crypt key of the store, for processing data, including point data, which is transmitted from outside of said memory of said IC card, and encrypted by said crypt

key of the store using said crypt key of said IC card, and for managing access to a point storage area corresponding to the store based on a register store number corresponding to the store (see column 2, lines 1-17; column 3, lines 59-65, column 8, lines 25-31). Takaragi does not teach the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically judged, the predetermined number of points is converted into a number, which is then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Tanager's IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 23, Takaragi et al teach:

A method of issuing point data to an IC card, the method comprising the steps of:

permitting said IC card to be inserted into a reader and writer, which has a crypt key of a store for encrypting data and a register store number for identifying the store, both of said register store number and said crypt key of the store being peculiar to the

store (see column 1, lines 65-67 – column 2, lines 1-30). Takaragi does not expressly mention a register store number corresponding to a store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not allowed to make reference to the transactions of other stores. And lines 59-67 of column 3 and figure 6, item 117 teach that each transaction area has a different authentication code that is used by each different store to access their specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that each transaction area has a unique authentication code that would function as the register store number corresponding to a store. This feature, in

combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from other stores.

Takaragi teaches wherein said IC card includes a memory having a plurality of storage areas, each of which stores point data, and a point management application, having a crypt key corresponding to said crypt key of the store, *wherein each point storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key* (see figure 1B; column 1, lines 65-67 – column 2, lines 1-30); and

transmitting to said IC card point data encrypted by said crypt key of the store, and decrypting the encrypted point data by said point management application using said crypt key of the point management application and allowing access to one of said point storage areas, which corresponds to the store, based on a register store number corresponding to the store (see column 2, lines 1-25; column 3, lines 55-67 – column 4, lines 1-12). Takaragi does not teach of the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically judged, the predetermined number of points is converted into a number, which is then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Tanager's IC card stores account balances (see column 4,

lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 24, Takaragi et al teach

A method of transmitting point data to an IC card with a reader and writer of a store, the method comprising the steps of:

permitting said IC card to be set into said reader and writer of the store which is uniquely assigned the crypt key of a store for encrypting data and a register store number for identifying the store, said IC card including a memory which has plurality of point storage areas for storing said point data, and a point management application, having a crypt key corresponding to said crypt key of the store, for processing said point data and managing access to a point storage area corresponding to the store based on a register store number corresponding to the store, *wherein each point storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key* (see column 1, lines 65-67 – column 2, lines 1-30; column 3, lines 55-67). Takaragi does not expressly mention a register store number corresponding to the store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not

allowed to make reference to the transactions of other stores. And lines 59-67 of column 3 and figure 6, item 117 teaches that each transaction area has a different authentication code that is used by each store to access its specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that each transaction area would have a unique authentication code that would function as the register store number corresponding to a store. This feature, in combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from the other stores.

Takaragi teaches inputting to the IC card point data encrypted by said crypt key of the store, said point data being issued corresponding to a customer's use (see column 3, lines 60-67);

decrypting the encrypted point data by said point management application using said crypt key of the point management application (see column 2, lines 1-25; column 3, lines 59-67);

and storing the decrypted point data into said point storage area corresponding to the store based on said register store number corresponding to the store by said point management application (see column 3, lines 55-67). Takaragi does not teach the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically judged, the predetermined number of points is converted into a number, which is then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Tanager's IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 25, Takaragi et al teach:

A point management system comprising:

a point system management apparatus which registers a store which participates in a point system, and which provides the store with a register store number for identifying the store and crypt key of the store for encrypting data, which are peculiar to the store (see column 1, lines 65-67 – column 2, lines 1-30; column 3, lines 55-67). Takaragi does not expressly mention a register store number corresponding to a store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not allowed to make reference to the transactions of other stores. And lines 59-67 of column 3 and figure 6, item 117 teach that each transaction area has a different authentication code that is used by each store to access its specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from

among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that each transaction area has a unique authentication code that would function as the register store number corresponding to a store. This feature, in combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from the other stores.

Takaragi teaches an IC card having a memory which includes a plurality of point storage areas each storing point data which is assigned corresponding to a customer's use, and a point management application, having a crypt key corresponding to said crypt key of the store, for processing data, including point data encrypted by said crypt key, using said crypt key of the point management application, managing access to a point storage area corresponding to the store based on a register store number corresponding to the store and securing a point storage area to store point data of a new store if use of said IC card in the new store is a first time, *wherein each point storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key* (see column 2, lines 1-25; column 8, lines 25-31); and

a reading and writing apparatus, which reads and writes said IC card by using said register store number corresponding to the store and said crypt key of the store (see column 3, lines 50-67 – column 4, lines 1-15; column 7, lines 14-42, figure 6). Takaragi does not teach the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that

checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically judged, the predetermined number of points is converted into a number, which is then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Tanager's IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 26, Takaragi et al teach:

An IC card comprising:

a memory having a plurality of point storage areas storing point data which is assigned corresponding to a customer's use (see figure1B); and

a point management application, having a crypt key corresponding to a crypt key of a store, for processing data, including point data encrypted by said crypt key of the store, using said crypt key of said point management application, managing access to a point storage area corresponding to the store based on a register store number corresponding to the store, and securing a point storage area to store point data of a new store if use of said IC card in the new store is a first time, *wherein each point*

storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key (see column 2, lines 1-25, column 3, lines 55-67, column 8, lines 25-31). Takaragi does not expressly mention a register store number corresponding to a store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not allowed to make reference to the transactions of other stores. And lines 59-67 of column 3 and figure 6, item 117 teach that each transaction area has a different authentication code that is used by each store to access its specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that each transaction area has a unique

authentication code that would function as the register store number corresponding to a store. This feature, in combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from the other stores.

Takaragi does not teach the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically judged, the predetermined number of points is converted into a number, which is then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Tanager's IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 27, Takaragi et al teach:

A point management system comprising:

point system management apparatus which registers stores which participate in a point system, and which provides each of the stores with a register store number, and

a crypt key which are peculiar to the store, and which controls a plurality of said stores as a group and provides to the group of stores a group number which is peculiar to the group (see column 2, lines 1-25; see column 3, lines 59-65). Takaragi does not expressly mention a register store number corresponding to a store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not allowed to make reference to the transactions of other stores. And lines 59-67 of column 3 and figure 6, item 117 teach that each transaction area has a different authentication code that is used by each store to access its specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that each transaction area would have a unique authentication code that

would function as the register store number corresponding to a store. This feature, in combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from the other stores.

Takaragi does not expressly teach a group transaction area where several stores would save their transaction data. However, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if Takaragi has different transaction areas in the same IC card, it would have a transaction area that would be used by several stores. The stores would have the same encipher key to access that area and would save their data in the same transaction area (see column 2, lines 17-25). This feature would help stores to share data between them.

Takaragi teaches an IC card having a memory having a plurality of point storage areas, each storing point data which is assigned by each of the stores corresponding to a customer's use and a group point storage area storing group point data which is assigned by the stores corresponding to a customer's use of a store in the group, and a point management application, having a crypt key corresponding to said crypt key of the store, for processing data, including point data encrypted by said crypt key of the store, using said crypt key of said point management application, managing access to a point storage area corresponding to the store based on a register store number corresponding to the store, and managing access to said group point storage area based on said group number and a reading and writing apparatus which reads and writes said IC card by using said register store number corresponding to the store, said group number and said crypt key of the store, *wherein each point storage area of a*

store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key (see column 2, lines 1-17; column 3, lines 59-65, column 8, lines 25-31). Takaragi does not teach the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically judged, the predetermined number of points is converted into a number, which is then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Tanager's IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 28, Takaragi teaches:

An IC card comprising:

a memory having a plurality of point storage areas storing point data which is assigned by stores each having a register store number and a crypt key which are peculiar to said store corresponding to a customer's use, and a group point storage area

storing group point data which is assigned by stores within a group of stores having a group number which is peculiar to the group corresponding to a customer's use of stores of the group, *wherein each point storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key* and point management application, having a crypt key corresponding to said crypt key of the store, for processing data, including point data encrypted by said crypt key, using said crypt key of said point management application, managing access a point storage area based on a register store number corresponding to the store and managing access to said group storage area based on said group number (see column 2, lines 1-25; see column 3, lines 59-65). Takaragi does not expressly mention a register store number corresponding to a store. However, lines 20-25 of column 1 teach that the IC card has transaction areas that are different depending upon the store, so that one store is not allowed to make reference to the transactions of other stores. And lines 59-67 of column 3 and figure 6, item 117 teach that each transaction area has a different authentication code that is used by each store to access its specific transaction area. Also, Takaragi teaches in column 2, lines 5-24 teaches "The IC card administrator assigns an encipher key code and a decipher key code for each of the transaction areas, writes an available upper-limit amount of money and the encipher key code or the decipher key code on a portion of the corresponding transaction area, and encrypts the transaction area using the encipher key. The IC card administrator hands the IC card over to the user. The IC card administrator further hands the encipher keys and the decipher keys to the

respective individual stores so that they can encrypt and decipher the transaction areas. Owing to the above mentioned procedures different encipher keys and decipher keys are held by the different stores. Therefore, a given store is permitted to process only the transaction areas that correspond to the encipher key and the decipher key held by that store from among the plurality of transactions areas contained in the IC card". Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that each transaction area would have a unique authentication code that would function as the register store number corresponding to a store. This feature, in combination with the encipher codes that are also different for each store (see column 8, lines 25-30), would keep the information from one store secret from the other stores.

Takaragi does not expressly teach a group transaction area where several stores would save their transaction data. However, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if Takaragi has different transaction areas in the same IC card, it would have a transaction area that would be used by several stores. The several stores would have the same encipher key to access that area and would save their data in the same transaction area (see column 2, lines 17-25). This feature would help stores to share data between them.

Takaragi does not teach the store of point data in the IC card. However, Mori teaches of an IC card that stores point data in an IC card and a point management system that checks if the number of points has reached a predetermined number. When the predetermined number of points has been reached, this state is automatically

judged, the predetermined number of points is converted into a number, which is then added to the pre-paid region of the card (see column 5, lines 35-45). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was made, to know that if the Tanager's IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

As per claim 29, Takaragi et al teach:

An IC card according to claim 22, wherein said point management application distinguishes data transmitted from a reading and writing apparatus of several stores and records points in an area within said plurality of point storage areas of said memory (see column 2, lines 1-30; column 8, lines 25-30).

As per claim 30, Takaragi et al teach:

An IC card according to claim 29, wherein said point management application allows access to an area that corresponds to transmitted data and prohibits access to other areas (see column 8, lines 25-30).

As per claim 31, Takaragi et al teach:

An IC card according to claim 29, wherein said point management application allows writing point data into an area that corresponds to transmitted data, and prohibits

writing to other areas, and reads point data from both an area that corresponds to transmitted data and another store's area (see column 3, lines 55-67 – column 4, lines 1-15; column 8, lines 25-31).

As per claim 32, Takaragi et al teach:

A point management system according to claim 25, wherein said point management application distinguishes data transmitted from a reading and writing apparatus of several stores and records points in an area them within said plurality of point storage areas of said memory (see column 2, lines 1-25; column 8, lines 25-31).

As per claim 33, Takaragi et al teach:

A point management system according to claim 32, wherein said point management application allows access to an area that corresponds to transmitted data and prohibits access to other areas (see column 8, lines 25-32).

As per claim 34, Takaragi et al teach:

A point management system according to claim 32, wherein said point management application allows writing point data into an area that corresponds to transmitted data, and prohibits writing to other areas, and reads point data from both an area that corresponds to transmitted data and another store's area (see column 3, lines 59-67 – column 4, lines 1-7; column 8, lines 25-31).

As per claim 35, Takaragi et al teach:

An IC card according to claim 22, wherein each of said point storage areas has a history storage area storing times of using said IC card in the store corresponding to said point storage area (see figure 3, item 61).

As per claim 36, Takaragi et al teach:

A point management system according to claim 25, wherein said point management application writes crypt key peculiar to the new store when securing the point storage area for the new store (see column 8, lines 25-31).

As per claim 37, Takaragi et al teach:

A point management system according to claim 25, wherein each of said point storage areas has a history storage area storing times of using said IC card in the store corresponding to said point storage area (see column 8, lines 25-31).

Claim 38 contains the same limitations as claim 21 therefore the same rejection is applied.

Claim 39 contains the same limitations as claims 21 and 22 therefore the same rejection is applied.

Claim 40 contains the same limitations as claim 36 therefore the same rejection is applied.

Claim 41 contains the same limitations as claim 36 therefore the same rejection is applied.

Claim 42 contains the same limitations as claim 27 therefore the same rejection is applied.

Claim 43 contains the same limitations as claim 27 therefore the same rejection is applied.

Claim 44 contains the same limitations as claim 27 therefore the same rejection is applied.

Response to Arguments

5. The Applicant's arguments filed on 08/05/04 have been fully considered but they are not persuasive. The Applicant argues that Takagari does not teach the Applicant's invention because the Takaragi method is time consuming and possibly faulty. The Applicant also argues that his claimed invention overcomes the prior art Takaragi because his claimed invention access the point storage area without the need for deciphering the point data stored in the storage area.

The Examiner answers that when given their broadest reasonable interpretation, the claims on examination sweep in the prior art, and the prior art, which are Takaragi and Mori, would have directed an artisan of ordinary skill to make the rejection cited by the examiner. The Applicant is arguing about features that are not in the claims when he argues that the Takaragi system is more time consuming compare to the Applicant's system and that that his claimed invention overcomes the prior art Takaragi because his claimed invention access the point storage area without the need for deciphering the point data stored in the storage area. Applicant claim 21 recites "*wherein each point storage area of a store is formed in corresponding relation to a register store number of the store to permit the point storage area of the store to be accessed using the register store number and a crypt key.* Takaragi teaches the use of an unique crypt key and an unique register store number for each store, as explained in the above rejection of claim 21, for the purpose of accessing the different transactions areas held by the different stores. Mori teaches an IC card that stores and manages point data. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the application was

made, to know that if the Takaragi IC card stores account balances (see column 4, lines 63-67 – column 5, lines 1-15), it would also store point data, as taught by Mori. Each store would have a different transaction area in the Takaragi card and would store the balance and amount of points accumulated for that particular store. The granting of points would be an incentive for customers to use the Takaragi card as every purchase would increase the number of points that would be used to redeem awards or to receive credits.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANIEL LASTRA whose telephone number is 703-306-5933. The examiner can normally be reached on 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, ERIC W STAMBER can be reached on 703-305-8469. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DL

Daniel Lastra
October 23, 2004

JAMES W. MYHRE
PRIMARY EXAMINER